

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Contrôle des assurés sociaux et profilage dans le secteur public

Degrave, Élise

Published in:
Journal des Tribunaux

Publication date:
2015

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Degrave, É 2015, 'Contrôle des assurés sociaux et profilage dans le secteur public', *Journal des Tribunaux*, Numéro 6610, p. 517-519.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La technique du profilage permet ainsi d'identifier des caractéristiques passées, présentes et futures d'un individu, caractéristiques dont on n'a pas la preuve concrète, mais pour lesquelles l'outil de profilage indique qu'il existe une forte présomption qu'elles existent. Cette identification est faite de manière plus fine que si elle était réalisée par des agents de l'administration, l'outil de profilage pouvant dépasser les compétences humaines en effectuant de multiples corrélations entre les données très nombreuses qui sont traitées⁶. La technique du profilage est également plus rapide, et donc moins coûteuse, que la sollicitation des agents.

Au-delà de son efficacité, l'utilisation du profilage dans le secteur public présente des risques. Le nombre de données traitées en provenance de l'ensemble des administrations est tellement important que des erreurs sont inévitables. Or ces erreurs peuvent avoir un impact important, puisque l'individu dont le profil est affecté d'une erreur sera assimilé à une catégorie de la population qui ne lui correspond pas en réalité. Il sera alors soumis, parfois à de multiples reprises, à des décisions discriminatoires qui le privent injustement de biens ou de services auxquels il aurait pu prétendre sans cette erreur⁷.

2 Le profilage des employeurs via l'outil OASIS

À l'heure actuelle, l'administration belge recourt déjà au profilage dans le cadre de la lutte contre la fraude sociale, pour cibler les fraudes opérées par les employeurs. Pour ce faire, un entrepôt de données qui répond au nom exotique d'« OASIS »⁸ a été créé. Ce système est opérationnel depuis 2005⁹. OASIS regroupe un grand nombre de données relatives aux employeurs et aux travailleurs¹⁰ du secteur de la construction et de l'horeca, notamment¹¹. Les données traitées sont des données de sécurité sociale et de données fiscales, essentiellement¹². Elles sont fournies notamment par l'O.N.S.S., l'O.N.E. et le S.P.F. Finances¹³ et transitent par la Banque-carrefour de la sécurité sociale, cette dernière jouant un rôle clé dans le fonctionnement d'OASIS¹⁴. Des réflexions sont en cours pour étendre OASIS à d'autres secteurs et d'autres données¹⁵.

Lors d'une opération de profilage, on applique aux données enregistrées dans OASIS un certain nombre d'alarmes, qui sont des algorithmes de détection de fraude mettant en relation des données déterminées. Si une alarme se déclenche au sujet d'un employeur, cela signifie que celui-ci est suspect au regard du type de fraude traité par l'alarme et les inspecteurs sociaux seront incités à le contrôler. Des fraudes diverses peuvent ainsi être plus facilement détectées, telles que les chantiers non déclarés, les travailleurs non déclarés, les abus en matière de chômage temporaire, etc.

L'outil OASIS souffre d'une faille majeure dans notre État de droit. Il n'est encadré par aucun texte légal ni même réglementaire. Aucun débat démocratique n'a pu être mené quant à son existence et son fonctionnement et on ignore si des garanties existent pour les citoyens, en termes de contrôle et de transparence notamment. On peut donc raisonnablement craindre que cet outil, mis en place par l'administration, soit très fortement orienté vers l'efficacité administrative, sans tenir compte suffisamment des libertés citoyennes.

Cette situation est inconstitutionnelle. OASIS constitue une évidente ingérence dans la vie privée des citoyens. Il regroupe un grand nombre de données à caractère personnel des citoyens, issues des bases de données de l'administration, appelées « sources authentiques de données ». Ces informations ont été initialement collectées par les administrations pour l'exécution de missions légales déterminées, telles que le paiement des allocations aux bénéficiaires, et non dans le but de les soumettre à des opérations de profilage. OASIS réutilise donc des données dans un but de contrôle différent de celui poursuivi lors de la collecte de ces informations, et ce sans en informer les personnes concernées. En outre, le *data mining* est un traitement de données puissant qui présente intrinsèquement des dangers. Or, par application de l'article 22 de la Constitution qui consacre le droit à la vie privée de chaque individu, toute ingérence dans la vie privée doit être organisée par une loi au sens formel du terme. Un débat démocratique est nécessaire pour réfléchir à la concrétisation, dans l'utilisation d'OASIS, du délicat équilibre entre efficacité administrative et vie privée. En outre, pour répondre au prescrit de la Convention européenne des droits de l'homme¹⁶, de la directive 95/46 en matière de traitements de données à caractère personnel¹⁷ et de la Convention n° 108¹⁸, la loi qui encadrera OASIS doit être suffisamment claire. Elle doit fixer précisément les éléments essentiels de l'ingérence, c'est-à-dire, les balises encadrant l'usage d'OASIS (finalités du traitement mis en œuvre, données utilisées, destinataires des données, obligation d'informer personnes concernées de cet usage de leurs données, contrôle de l'outil, etc.)¹⁹.

Le manque d'encadrement légal d'OASIS est également contraire à plusieurs textes internationaux. Ainsi, la résolution de Varsovie²⁰ prévoit notamment que « les commissaires [à la protection des données] demandent (...) aux gouvernements du monde entier de garantir la transparence et de donner à la population et aux parties prenantes la possibilité d'exprimer leur point de vue dans le cadre de tout processus lié à l'adoption de lois prévoyant la mise en place d'activités de profilage ». Par ailleurs, l'importante recommandation du Conseil de l'Europe sur le profilage²¹ insiste également sur la nécessité d'une loi qui doit organiser clairement un profilage loyal et prévoir des garanties pour les personnes concernées.

national Journal of Law and Information Technology, 2001, vol. 9, n° 1, pp. 62-63 ; J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, « L'application de la Convention 108 au mécanisme de profilage - Éléments de réflexion destinés au travail futur du comité consultatif », mars 2008, T-PD (2008) 01, p. 5.

(6) M. SAINTRAIN, « T.I.C., nouveaux standards transactionnels et fiscalité », Bureau du Plan, working paper, 15-03, août 2003, pp. 41 et 42 ; J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *op. cit.*, p. 9 ; V. PAPAKONSTANTINO, *op. cit.*, p. 47 ; projet de loi « relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances », *Doc. parl.*, Chambre, sess. 2006-2007, n° 51 3064/001, pp. 73-74.

(7) Recommandation CM/Rec(2010)13 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010. Voy. également le point 72 de l'exposé de motifs de cette recommandation.

(8) « OASIS » est l'abréviation des termes « organisation antifraude des services d'inspection sociale ».

(9) Compte rendu analytique de la commission des affaires sociales, *Doc. parl.*, Chambre, sess. 2004-2005, COM 541, p. 19.

(10) Selon le comité sectoriel de la sécurité sociale, les données relatives aux travailleurs sont enregistrées dans OASIS « afin d'offrir aux inspecteurs sociaux une meilleure vue d'ensemble des employeurs » [comité sectoriel de la sécurité sociale, délibération n° 05/001, *op. cit.*, p. 4].

(11) Délibération n° 01/06 du 6 mars 2001 relative à une demande du ministère fédéral des Affaires sociales, de la Santé publique et de l'Environnement pour la création et la gestion d'une banque de données OASIS en vue de la lutte contre la fraude sociale dans les secteurs de la construction, de la construction métallique, de l'électricité et des parcs et jardins, p. 1 ; délibération n° 05/001 du 18 janvier 2005 relative à la création et gestion de la banque de données OASIS en vue de la lutte contre la fraude sociale ; délibération n° 01/06 du 6 mars 2001, extension de l'autorisation, p. 4.

(12) Voy. comité sectoriel de la sécurité sociale, délibération n° 01/06, *op. cit.*, p. 1, note 1 ; C.P.V.P., recommandation n° 01/2012 du 18 janvier 2012 concernant la possibilité d'un inventaire des banques de données

pertinentes et d'une amélioration de l'échange d'informations dans le cadre de la lutte contre la fraude sociale, pp. 5 et 6 ; L.-A. TAUFLER, « The Datawarehouse OASIS », 1^{er} février 2008, disponible sur le site <http://litpc45.ulb.ac.be/OasisWorkshop/tauflier.pdf> ; entretien avec un fonctionnaire de l'administration fédérale, le 17 juin 2008.

(13) Pour de plus amples détails au sujet des données contenues dans OASIS, voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée - Légalité, transparence et contrôle*, Bruxelles, Larcier, coll. C.R.I.D.S., 2014, pp. 72 et s.

(14) Voy. https://www.ksz-bcss.fgov.be/fr/bcss/services/content/websites/belgium/services/service_institution/service_regional/service_26.html.

(15) Pour une présentation d'OASIS et ses perspectives, voy. <http://social-security.fgov.be/projects/thedata-mentalists/index.html>.

(16) Article 8 de la Convention européenne des droits de l'homme.

(17) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre cir-

culcation de ces données

(18) Convention du Conseil de l'Europe 108 du 28 janvier 1981 pour la protection des personnes à l'égard des traitements automatisés des données à caractère personnel.

(19) Pour de plus amples informations à ce sujet, voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, spécialement pp. 133 et s. et références citées.

(20) Résolution sur le profilage de Varsovie, 23-26 septembre 2013, disponible sur le site de la Commission de la protection de la vie privée, <http://www.privacycommission.be/sites/privacycommission/files/documents/Profiling-resolution.pdf>. Voy. également la déclaration d'Uruguay sur le profilage, 26 octobre 2012 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/12-10-26_Uruguay_Declaration_Profiling_EN.pdf.

(21) Recommandation CM/Rec(2010)13 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 23 novembre 2010.

3 Le profilage des assurés sociaux

Avec le plan d'action 2015, une étape supplémentaire est franchie dans le déploiement du profilage dans le secteur public. Ce sont à présent les assurés sociaux qui seront soumis au *data mining*, à partir des données à caractère personnel qu'ils auront communiquées aux administrations, mais également à leurs fournisseurs d'énergie. Le plan d'action 2015 l'affirme explicitement, qualifiant le projet de *data mining* de l'assuré social⁽²²⁾. Vu qu'il s'agit d'un projet de lutte contre la fraude sociale impliquant l'intervention de la Banque-carrefour de la sécurité sociale, on peut raisonnablement penser qu'à terme, OASIS sera utilisé également pour effectuer le *data mining* des assurés sociaux.

Au-delà du fait qu'il est profondément dérangeant que l'extension d'une technique aussi intrusive que le profilage soit réalisée au départ de la sphère intime des personnes socialement défavorisées, il importe de prévenir le législateur du travail considérable qui l'attend dans ce dossier.

Tout comme il importe de le faire pour l'outil OASIS, le profilage des assurés sociaux doit être minutieusement encadré par le législateur qui doit en définir les éléments essentiels, par application de l'article 22 de la Constitution et du régime juridique de la protection des données à caractère personnel⁽²³⁾.

Ainsi, la finalité des traitements appliqués aux données des assurés sociaux doit être clairement déterminée. À cette occasion, il y a lieu de mentionner explicitement dans la loi l'utilisation de la technique du profilage, et l'utilisation d'OASIS le cas échéant, de manière à ce que chacun puisse avoir connaissance de ces traitements de données.

En outre, le législateur doit identifier les données adéquates et pertinentes qui serviront de base au profilage. À cette fin, il y a lieu de déterminer des seuils de consommation d'énergie en dessous ou au-dessus desquels une domiciliation fictive sera suspectée. Or est-il possible de définir de tels seuils à partir des données de gaz, d'eau et d'électricité ? On en doute fortement⁽²⁴⁾ vu la difficulté d'établir une moyenne de consommation énergétique par ménage⁽²⁵⁾. En effet, trop de facteurs distincts déterminent la consommation d'énergie, particulièrement dans les milieux sociaux défavorisés. Cette consommation peut y être fortement influencée par la vétusté du bâtiment, la piètre isolation de celui-ci, le type d'équipement ou encore la précarité de l'assuré social qui le contraint d'économiser le gaz, l'eau et l'électricité.

Par ailleurs, le plan d'action 2015 prévoit d'obliger les fournisseurs d'énergie à communiquer automatiquement leurs données à la Banque-carrefour de la sécurité sociale, en vue de les soumettre au *data mining*⁽²⁶⁾. Faut-il comprendre par là que les données de tous les clients de chaque fournisseur d'énergie vont être communiquées ? C'est particulièrement problématique au regard de l'obligation de n'utiliser que les données strictement nécessaires au regard de la finalité poursuivie. Cela signifierait que les données de chacun seraient transmises alors même qu'il n'y a aucun indice de risque de domiciliation fictive et que les personnes visées ne font peut-être même pas partie de la catégorie des assurés sociaux. De plus, il n'est pas nécessaire de communiquer l'information en entier. Le même objectif peut être atteint en ne réclamant que la réponse selon laquelle « oui » ou « non », la personne concernée dépasse tel seuil de consommation (si tant est qu'on ait réussi à le définir...).

Une attention particulière doit aussi être portée à la transparence de ces traitements de données à l'égard des personnes concernées. Chacun a le droit de savoir ce qui est détenu à son sujet, ne fût-ce que pour corriger les erreurs qui affecteraient ses données à caractère personnel. C'est particulièrement important dans le contexte opaque de l'e-gouvernement où les données sont réutilisées un maximum de fois et où

toute erreur aura un effet domino. Pour répondre au prescrit du régime juridique de la protection des données à caractère personnel, la mise en œuvre du profilage devrait donc notamment s'accompagner de la création d'un portail internet sur lequel la personne concernée aurait la possibilité de s'identifier à l'aide de sa carte d'identité électronique. Elle devrait ensuite pouvoir consulter aisément les données enregistrées à son sujet, leur localisation dans l'administration, découvrir qui les a consultées, quels échanges de données ont déjà eu lieu. En cas de profilage, la personne devrait également pouvoir obtenir les informations nécessaires pour comprendre la logique qui sous-tend la décision informatisée de lui attribuer tel profil⁽²⁷⁾. Le portail devrait également offrir la possibilité d'exercer, en ligne, le droit de rectification des données erronées, le cas échéant.

Enfin, le législateur devrait désigner une autorité indépendante chargée du contrôle efficace des opérations de profilage, et ce avant et pendant leur mise en œuvre. Cette autorité devrait également pouvoir vérifier à intervalles réguliers la pertinence et la mise à jour des données utilisées et disposer de moyens d'action pour obtenir la cessation des abus éventuels.

Conclusions

Le profilage dans le secteur public, en particulier lorsqu'il vise les assurés sociaux, constitue un bouleversement dans la relation entre les citoyens et l'administration. Une réflexion en profondeur doit être menée pour éviter un déséquilibre inacceptable entre la puissance technologique de l'administration et les prérogatives des citoyens, spécialement lorsqu'ils se trouvent dans une situation sociale difficile. En somme, c'est l'idée que « within a democracy, citizen should not be left as pedestrians when the authorities drive limousines »⁽²⁸⁾.

Certes, le déséquilibre entre l'administration et le citoyen n'est pas propre à l'utilisation des technologies. Il existe depuis longtemps une inégalité fondamentale entre l'administration « qui doit faire prévaloir l'intérêt général, et l'administré, qui ne défend en général que son intérêt personnel »⁽²⁹⁾. Organiser une stricte égalité entre les droits et les devoirs de l'administration et du citoyen est d'ailleurs inconcevable, car elle « impliquerait l'abolition de la forme étatique elle-même »⁽³⁰⁾.

Néanmoins, l'utilisation des technologies au sein de l'administration risque d'accentuer fortement ce déséquilibre. L'enregistrement de multiples données des citoyens et les outils permettant notamment le profilage renforcent la puissance de l'administration, qui est à présent en mesure d'avoir une connaissance précise de chaque individu. Dans le même temps, l'action de l'administration informatisée est plus opaque, compte tenu de la difficulté pour le citoyen de savoir ce que l'administration détient sur lui et de comprendre l'usage qui est fait de ses informations. Dans ce contexte, on peut craindre que l'administration agisse comme un *Big Brother* qui surveille chaque individu. Plus fondamentalement, une administration kafkaïenne, distante, incompréhensible, incontrôlable risque d'émerger.

Il devient urgent d'attribuer à chacun les moyens d'exercer une prise sur l'administration, pour la comprendre et la contrôler, notamment en dénonçant les abus éventuels dans l'utilisation des données à caractère personnel qui la conduiraient à prendre des décisions discriminatoires. Gageons du fait qu'à l'heure où vont s'engager d'importantes discussions sur le profilage des assurés sociaux, le législateur saura être attentif à cet enjeu fondamental pour l'avenir de notre État de droit.

Elise DEGRAVE

Chargée de cours à la Faculté de droit de l'Université de Namur
Post-doctorante à la chaire E-Gouvernement et au C.R.I.D.S.

(22) Voy. plan d'action 2015, p. 33. Voy. dans le même sens p. 39.

(23) On vise par là l'article 8 de la Convention européenne des droits de l'homme, la directive 95/46 précitée et la Convention n° 108 précitée.

(24) La Commission de la protection de la vie privée abonde dans le même sens, dans un avis rendu à propos d'un projet semblable datant de la législature précédente. Voy. C.P.V.P. avis n° 06/2012 du 6 février 2012.

2012 sur un avant-projet de loi programme en ce qui concerne la lutte contre la fraude et plus particulièrement le contrôle sur l'abus des adresses fictives par les assurés sociaux, n° 12.

(25) Sibelga, *Energiguide.be*, « Quelle est la consommation moyenne d'énergie et de gaz en Région bruxelloise ? ». Voy. également X. MAY, *Analyse de la facture énergétique des ménages et mesures des dif-*

ficultés rencontrées par les personnes âgées, U.L.B.-S.P.F. Économie, octobre 2013, disponible à l'adresse http://economie.fgov.be/fr/binaries/Analyse_facture_energetique_difficultes_personnes_agees_tcm326-252357.pdf

(26) Plan d'action social 2015, p. 39. (27) Voy. notamment article 10, c), de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à

caractère personnel.

(28) D.W. SCHARTUM, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology*, 1998/1, § 7.1.

(29) A. MAST, A. ALLEN et J. DUJARDIN, *Précis de droit administratif*, Bruxelles, Story-Scientia, 1989, p. 5.

(30) J. CHEVALLIER, « Le droit administratif, un droit de privilège ? », *Pouvoirs*, 1988, n° 46, p. 67.